

information has occurred. The Senior Component Official for Privacy, or their designee, shall notify the Defense Privacy Office of the breach within 48 hours upon being notified that a loss, theft, or compromise has occurred. The notification shall include the following information:

(i) Identify the Component/organization involved.

(ii) Specify the date of the breach and the number of individuals impacted, to include whether they are DoD civilian, military, or contractor personnel; DoD civilian or military retirees; family members; other Federal personnel or members of the public, etc.

(iii) Briefly describe the facts and circumstances surrounding the loss, theft, or compromise.

(iv) Briefly describe actions taken in response to the breach, to include whether the incident was investigated and by whom; the preliminary results of the inquiry if then known; actions taken to mitigate any harm that could result from the breach; whether the affected individuals are being notified, and if this will not be accomplished within 10 working days, that action will be initiated to notify the Deputy Secretary (see § 310.14); what remedial actions have been, or will be, taken to prevent a similar such incident in the future, e.g., refresher training conducted, new or revised guidance issued; and any other information considered pertinent as to actions to be taken to ensure that information is properly safeguarded.

(2) The Component shall determine whether administrative or disciplinary action is warranted and appropriate for those individuals determined to be responsible for the loss, theft, or compromise.

### Subpart L—Computer Matching Program Procedures

#### § 310.51 General.

(a) A computer matching program covers two kinds of matching programs (see OMB Matching Guidelines, 54 FR 25818 (June 19, 1989)). If covered, the matches are subject to the requirements of this subpart. The covered programs are:

(1) Matches using records from Federal personnel or payroll systems of records, or

(2) Matches involving Federal benefits program if:

(i) To determine eligibility for a Federal benefit,

(ii) To determine compliance with benefit program requirements, or

(iii) To effect recovery of improper payments or delinquent debts under a Federal benefit program.

(b) The requirements of this part do not apply if matches are:

(1) Performed solely to produce aggregated statistical data without any personal identifiers. Personally identifying data can be used for purposes of conducting the match. However, the results of the match shall be stripped of any data that would identify an individual. Under no circumstances shall match results be used to take action against specific individuals.

(2) Performed to support research or statistical projects. Personally identifying data can be used for purposes of conducting the match and the match results may contain identifying data about individuals. However, the match results shall not be used to make a decision that affects the rights, benefits, or privileges of specific individuals.

(3) Performed by an agency, or a component thereof, whose principal function is the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named individual or individuals.

(i) The match must flow from an investigation already underway which focuses on a named person or persons. “Fishing expeditions” in which the subjects are generically identified, such as “program beneficiaries” are not covered.

(ii) The match must be for the purpose of gathering evidence against the named individual or individuals.

(4) Performed for tax information-related purposes.

(5) Performed for routine administrative purposes using records relating to Federal personnel.

(i) The records to be used in the match must predominantly relate to Federal personnel (i.e., the percentage of records in the system of records that

## Office of the Secretary of Defense

## § 310.53

are about Federal personnel must be greater than of any other category).

(ii) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(6) Performed using only records from systems of records maintained by an agency.

(i) The purpose of the match must not be for purposes of taking any adverse financial, personnel, disciplinary, or other unfavorable action against an individual.

(ii) A match of DoD personnel using records in a system of records for purposes of identifying fraud, waste, and abuse is not covered.

(7) Performed to produce background checks for security clearances of Federal or contractor personnel or performed for foreign counter-intelligence purposes.

### § 310.52 Computer matching publication and review requirements.

(a) DoD Components shall identify the systems of records that will be used in the match to ensure the publication requirements of subpart G have been satisfied. If the match will require disclosure of records outside the Department of Defense, Components shall ensure a routine use has been established, and that the publication and review requirements have been met, before any disclosures are made (see subpart G of this part).

(b) If a computer matching program is contemplated, the DoD Component shall contact the DPO and provide information regarding the contemplated match. The DoD DPO shall ensure that any proposed computer matching program satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)).

(c) A computer matching agreement (CMA) shall be prepared by the Component, consistent with the requirements of § 310.53 of this subpart and submitted to the DPO. If the CMA satisfies the requirements of the Privacy Act (5 U.S.C. 552a) and OMB Matching Guidelines (54 FR 25818 (June 19, 1989)), as well as this subpart, it shall be forwarded to the

Defense Data Integrity Board (DIB) for approval or disapproval.

(1) If the CMA is approved by the DIB, the DPO shall prepare and forward a report to both Houses of Congress and to OMB as required by, and consistent with, OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996, as amended. Congress and OMB shall have 40 days to review and comment on the proposed match. Any comments received must be resolved before matching can take place.

(2) If the CMA is approved by the DIB, the DPO shall prepare and forward a match notice as required by OMB Circular A-130, "Management of Federal Information Resources," February 8, 1996, as amended, for publication in the FEDERAL REGISTER. The public shall be given 30 days to comment on the proposed match. Any comments received must be resolved before matching can take place.

### § 310.53 Computer matching agreements (CMAs).

(a) If a match is to be conducted internally within DoD, a memorandum of understanding (MOU) shall be prepared. It shall contain the same elements as a CMA, except as otherwise indicated in paragraph (b)(4)(ii) of this section.

(b) A CMA shall contain the following elements:

(1) *Purpose.* Why the match is being proposed and what will be achieved by conducting the match.

(2) *Legal authority.* What is the Federal or state statutory or regulatory basis for conducting the match. The Privacy Act does not constitute independent authority for matching. Other legal authority shall be identified.

(3) *Justification and expected results.* Explain why computer matching as opposed to some other administrative means is being proposed and what the expected results will be, including a specific estimate of any savings (see paragraph (b)(13) of this section).

(4) *Records description.* Identify:

(i) The system of records or non-Federal records. For DoD systems of records, provide the FEDERAL REGISTER citation for the system notice;